The Data Privacy Act of 2012
Impact and Significance
To non-life INSURANCE SECTOR

RAYMUND ENRIQUEZ LIBORO
PRIVACY COMMISSIONER AND CHAIRMAN
2016 – Awareness
2017 – Compliance
2018 – Enforcement
RESILIENCE AND THE FILIPINO SPIRIT
May 27, 2010

REPUBLIC ACT NO. 10121

AN ACT STRENGTHENING THE PHILIPPINE DISASTER RISK REDUCTION AND MANAGEMENT SYSTEM, PROVIDING FOR THE NATIONAL DISASTER RISK REDUCTION AND MANAGEMENT FRAMEWORK AND INSTITUTIONALIZING THE NATIONAL DISASTER RISK REDUCTION AND MANAGEMENT PLAN, APPROPRIATING FUNDS THEREFOR AND FOR OTHER PURPOSES

SECTION 1. Title. — This Act shall be known as the "Philippine Disaster Risk Reduction and Management Act of 2010".

SECTION 2. Declaration of Policy. — It shall be the policy of the State to:

(a) Uphold the people's constitutional rights to life and property by addressing the root causes of vulnerabilities to disasters, strengthening the country's institutional capacity for disaster risk reduction and management and building the resilience of local communities to disasters including climate change impacts;
RESILIENCE AND THE FILIPINO SPIRIT
Resilience

- Resilience
- rɪˈzɪliəns/
- noun
  - the capacity to recover quickly from difficulties; toughness.
  - adapt well to change
  - keep going in the face of adversity
21st Century Hazards and Risks

Norse – Superior Attack Intelligence

Norse maintains the world’s largest dedicated threat intelligence network. With over eight million sensors that span over six thousand applications – from Apple laptops, to ATM machines, to critical infrastructure systems, to closed-circuit TV cameras – the Norse Intelligence Network gathers data on who the attackers are and what they’re after. Norse delivers threat data through the Norse Appliance, which preemptively blocks attacks and improves your overall security ROI, and the Norse Intelligence Service, which provides professional continuous threat monitoring for large networks.

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Attacker IP</th>
<th>Attacker Geo</th>
<th>Target Geo</th>
<th>Attack Type</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>14:56:20.770</td>
<td>122.3.47.120</td>
<td>Paranaque, PH</td>
<td>Lynnwood, US</td>
<td>telnet</td>
<td>23</td>
</tr>
<tr>
<td>15:05:41.557</td>
<td>122.54.132.220</td>
<td>Makati, PH</td>
<td>Dubai, AE</td>
<td>telnet</td>
<td>23</td>
</tr>
<tr>
<td>15:04:02.333</td>
<td>122.3.47.120</td>
<td>Paranaque, PH</td>
<td>Lynnwood, US</td>
<td>telnet</td>
<td>23</td>
</tr>
</tbody>
</table>
The Data Privacy Act of 2012

A 21st Century Law

For 21st Century Rights and Risks
What is a Privacy Risk?

A Personal Data Breach or a Data Privacy Violation that has NOT happened yet.
What is Privacy Resilience?

A Personal Data Breach or a Data Privacy Violation that was prevented.

A breach and privacy disaster that did not happen.
Disaster
Resilience
DPA and the Philippine Development Plan

"Patuloy na Pag-Unlad" 
Increasing Growth Potential

Technology adoption promoted and accelerated Innovation stimulated

Creative capacity for knowledge and technology generation, acquisition and adoption enhanced

Ensure world class data privacy standards established in the country

"Pagbabago" 
Inequality-reducing Transformation

Expanding Economic Opportunities in Industry and Services through Trabaho at Negosyo

Consumer access to safe and quality goods and services ensured

Culture of Privacy and Privacy Resilience established in the country

"Malasakit" 
Enhancing the Social Fabric

Ensuring People-Centered, Clean, and Efficient Governance

Citizenry fully engaged and empowered

Empowered Data Subjects
THE PRIVACY COMMISSIONER

Philosophy

Risk management approach | Prevention and mitigation | Building the culture of data privacy and protection
Data Protection

- Confidentiality
- Availability
- Integrity
  - Compliance

Data Privacy

- Accountability
- Assurance
- Operational Compliance (culture of privacy)
  - Demonstrable Compliance

Personal Information
What the law is all about

How it will affect you
Impact of a Problematic Data Action on Business

• Loss of reputation
• Loss of market share
• Legal liabilities
ROOT CAUSES OF BREACH

- Malicious or criminal attack: 47%
- System Glitch: 29%
- Human Error: 24%

Insurance Company Fined $6.8 Million for Data Breach

The fine is in response to the exposure of data belonging to 13,336 of TSS' Dual Eligible Medicare beneficiaries.

On September 20, 2013, TSS mailed a pamphlet to approximately 70,000 Medicare Advantage beneficiaries that inadvertently showed some recipients' Medicare Health Insurance Claim Numbers, which are considered protected health information under the Health Insurance Portability and Accountability Act (HIPAA).

Following the discovery of the error, TSS reported the incident to state and federal authorities, offered financial assistance to all affected beneficiaries, and offered all those affected 12 months of free credit monitoring services.

"We take this matter very seriously and are working to prevent this type of incident in the future," TSS Health Management stated in a recent SEC filing regarding the fine.

In addition to the fine, all new enrollments of Dual Eligible Medicare beneficiaries will be required to voluntarily disenroll if they were affected will be offered the option to disenroll.

Photo courtesy of Shutterstock.
Large Insurance Company Settles for $5.5 Million over "Failed To Patch" Data Breach

Databases containing personal information being ‘hacked’ into or otherwise illegally accessed by individuals outside of the agency or organization
SINGAPORE - The personal data of 5,400 customers of AXA Insurance in Singapore was stolen due to a cyber attack.

The life insurance firm sent out an e-mail to most affected customers on Thursday, notifying them of the data breach. The remaining affected customers will be notified by the end of the week (Sept 8).

In the e-mail, AXA's data protection officer Eric Lehyon said: "We wish to inform you that on 10 Aug 2017 because of a recent cyber attack, personal data belonging to about 5,400 of our customers, past and present, on our Health Portal was compromised."


Databases containing personal information being ‘hacked’ into or otherwise illegally accessed by individuals outside of the agency or organization.
DATA PRIVACY RELATED DIFFICULTIES

- Customer database breaches
- Company’s lack of adequate policies to protect customer information
- Payment card security breaches
- Customer profiling leading to transparency concerns
PROCESSING PERSONAL INFORMATION CAN CREATE PROBLEMS FOR INDIVIDUALS

- Loss of trust
- Loss of self-determination
  - Loss of autonomy
  - Loss of liberty
  - Exclusion
  - Physical harm
- Discrimination
  - Stigmatization
  - Power imbalance
- Economic loss
AN 

introduction 

TO THE 

Data Privacy Act 

OF 2012
FULL TITLE

An act protecting individual personal information in information and communications systems in the government and the private sector, creating for this purpose a National Privacy Commission, and for other purposes
The National Privacy Commission protects individual personal information by regulating the processing of personal information. The law upholds the right to privacy by protecting individual personal information.
STRUCTURE OF RA 10173

Sections 1-6. Definitions and General Provisions

Sections 7-10. The National Privacy Commission

Sections 11-21. Rights of Data Subjects, and Obligations of Personal Information Controllers and Processors

Sections 22-24. Provisions Specific to Government

Sections 25-37. Penalties
The Privacy Ecosystem

YOU
The Data Subject

ORGANIZATIONS
Personal Information Controllers & Processors

REGULATORS
The NPC
SEC. 2. Protect the fundamental human right of privacy of communication while ensuring free flow of information to promote innovation and growth; role of information and communications technology to ensure that personal information under the custody of the government and private sector are secured.
BALANCE

Data Privacy

Free Flow

Information Privacy

Research

National Security and Public Safety

Right to Information

National Privacy Commission
SEC. 4. Applies to the processing of all types of personal information, in the country and even abroad, subject to certain qualifications.

SEC. 15. Personal information controllers may invoke the principle of privileged communication over privileged information that they lawfully control or process.
SCOPE OF THE LAW

- PERSONAL INFORMATION CONTROLLERS (PIC) and PERSONAL INFORMATION PROCESSORS (PIP) PROCESSING PERSONAL DATA of DATA SUBJECTS
Any operation of any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.
THE DATA LIFE CYCLE

CREATE AND COLLECT

STORE AND TRANSMIT

DISPOSE AND DESTROY

RETAIN

USE AND DISTRIBUTE
OBLIGATIONS OF A PERSONAL INFORMATION CONTROLLER

1. The PIC should collect personal information for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection.

2. The PIC should process personal information fairly and lawfully, and in accordance with the rights of a data subject.

3. The PIC should process accurate, relevant and up to date personal information.

4. The PIC should collect and process personal information adequately and not excessively.

5. The PIC should retain personal information only for as long as necessary for the fulfillment of the purposes for which the data was obtained. The information should be kept in a form which permits identification of data subjects for no longer than is necessary.

6. The PIC must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information.
Transparency
Legitimate Purpose
Proportionality
Security
Accountability
Data Privacy Principles
Security Measures
Uphold Rights of Data Subject
Choice
Notice
Access
Remedy
National Privacy Commission
DATA PRIVACY PRINCIPLES

NOTICE

TRANSPARENCY

LEGITIMATE PURPOSE

PROPORTIONALITY
Principle of Transparency

A data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.
Principle of Legitimate Purpose

The processing of information shall be compatible with a declared and specified purpose, which must not be contrary to law, morals, or public policy.
**Principle of Proportionality**

The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.
“PROPORTIONALITY”

PARA MAKAUTANG...
(PLEASE BRING THIS REQUIREMENTS)

- 6pcs 2x2 PICTURE
- 4pcs 1x1 PICTURE (WHOLE BODY)
- 3 VALID ID’S
- BRGY. CLEARANCE
- NBI CLEARANCE
- MAYORS PERMIT
- MEDICAL
- CEDULA
- BIRTH CERTIFICATE (NSO)
- SSS/TIN
- CO-MAKER
- X-RAY (WHOLE BODY)
- POLICE CLEARANCE
- PROOF OF BILLING
- FORM 137
THE FIVE

Pillars

of

Compliance
1. Commit to Comply: Appoint a **Data Protection Officer (DPO)**.

2. Know Your Risks: Conduct a **Privacy Impact Assessment (PIA)**.


4. Demonstrate Your Compliance: Implement your **privacy and data protection (PDP) measures**.

5. Be Prepared for Breach: Regularly exercise your **Breach Reporting Procedures (BRP)**.
When will you hear from the NPC?

1. When the NPC sends **advisories** and circulars
2. When the NPC **conducts audit and compliance checks**
3. When you **notify the NPC about a personal data breach**
What do we look for when the NPC comes knocking at your door?

1. Can we feel a culture of **Privacy**?
2. Do you have a **sensible data privacy program**?
3. Is it based on **risk assessment**?
4. Do you **train your staff in data privacy** and protection?
5. Are you prepared for **breach**?
The Data Privacy Golden Rule

If you Can’t Protect It...

DONT Collect It.
PRIVACY.GOV.PH

facebook.com/privacy.gov.ph
twitter.com/privacyph
info@privacy.gov.ph